AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of managing meta data using a central repository at a central repository subsystem, the central repository being accessible by a computing device through a communications network, the method comprising the steps of:

connecting to the central repository through the communications network based on a user input;

updating a local repository of the computing device with at least one segment from the central repository that is associated with the user to produce a meta data collection associated with the user; and

utilizing, by the computing device, the meta data collection during a current user session at the computing device to assist the user in using the computing device,

wherein the utilizing step comprises retrieving, from the meta data collection, meta data that would be most appropriate for each of different contexts of using the computing device, based on at least a current role ~~position~~ of the user.

2. (Original) The method of claim 1, further comprising the step of:

uploading any new segment from the computing device to the central repository at a predetermined time.

3. (Original) The method of claim 1, further comprising the step of:

incrementally uploading any new meta data generated during the current user session from the computing device to the central repository.

4. (Previously Presented) The method of claim 1, wherein the connecting step comprises:

receiving, by the central repository subsystem, authentication information from the user;

verifying validity of the authentication information; and

notifying the computing device that the user has proper authority to access the central repository if the authentication information is verified as valid.

5. (Previously Presented) The method of claim 4, wherein the authentication information comprises user identification, a pass phrase of the user, and an identifier for the central repository or a component at the central repository subsystem.

6. (Previously Presented) The method of claim 5, wherein the verifying step comprises: determining a secret key represented as a hash of:

the received user identification, concatenated with a hash of the received identifier, concatenated with the received pass phrase; and

comparing the secret key with a stored key associated with the user.

7. (Previously Presented) The method of claim 1, wherein the updating step comprises:

determining if the local repository is at a null state;

first requesting the central repository subsystem to transmit any segment associated with the user that has not been applied to the computing device if the determining step indicates that the local repository is not at a null state; and

second requesting the central repository subsystem to transmit all segments associated

with the user if the determining step indicates that the local repository is at a null state.

8. (Previously Presented) The method of claim 7, wherein the updating step further

comprises:

receiving at least one segment from the central repository subsystem in response to said

first requesting step;

decrypting the at least one segment; and

applying the decrypted at least one segment to the meta data collection to produce the

meta data collection associated with the user.

9. (Previously Presented) The method of claim 7, wherein the updating step further

comprises:

receiving at least one segment from the central repository subsystem in response to said

second requesting step;

decrypting the at least one segment; and

generating the meta data collection for the user using the decrypted at least one segment.

10. (Previously Presented) The method of claim 1, wherein the retrieving step is

performed using heuristics algorithms and the utilizing step further comprises applying the

retrieved meta data in each of the different contexts.

11. (Previously Presented) The method of claim 10, wherein the current context comprises at least one of the following: opening a web page, filling in a computer form, filling in a password-changing form, providing a certificate, opening a computer file, processing a computer file, or executing an application program.

12. (Previously Presented) The method of claim 10, wherein the utilizing step further comprises:

continuously collecting meta data resulting from use of the computing device during the current user session at the computing device; and

the method further comprises:

generating a new segment based on the collected meta data upon completion of the current user session; and

processing the new segment.

13. (Previously Presented) The method of claim 12, wherein the processing step comprises:

updating the meta data collection with the new segment.

14. (Previously Presented) The method of claim 12, wherein the meta data comprises application data for being usable in an application executable on the computing device, and context data for identifying context in which said application data are used, and

wherein the utilizing step further comprises:

determining statistical information associated with the meta data, the statistical

information indicating relationships between the meta data, wherein the retrieving step is

performed in part based on the statistical information.

15. (Original) The method of claim 14, wherein the context data identify at least one of

the following: user roles, uniform resource identifiers (URIs), file names, and/or form names

pertaining to the application data.

16. (Previously Presented) The method of claim 14, wherein the application data

comprise at least one of the following: page display setting data, file display setting data, user

ID/password combinations, field values for computer forms, user's preference data, bookmarks,

and certificates.

17. (Previously Presented) The method of claim 10, wherein the current context is for

filling in a computer form, and the applying step comprises:

automatically filling in the computer form with said most appropriate meta data.

18. (Previously Presented) The method of claim 10, wherein, if the current context is for

filling in a computer form, the utilizing step further comprises:

retrieving, from the meta data collection, alternative meta data that are related to the

current context of filling in the computer form; and

presenting the alternative meta data to the user for the user's consideration.

19. (Previously Presented) The method of claim 10, wherein the current context is for

filling in a password-changing computer form, and the retrieved meta data comprises a user

identification and a password, and

wherein the applying step comprises:

presenting to the user the password in an obfuscated format; determining whether

it is safe to present the actual password to the user; and

presenting the actual password in a non-obfuscated format when it is determined

to be safe to present the actual password.

20. (Previously Presented) The method of claim 1, wherein the utilizing step comprises:

formulating search requirements based on a current context of using the computing

device; and

executing a search based on the search requirements using heuristics algorithms.

21. (Original) The method of claim 20, wherein the search requirements specify weighted

properties of the current context of using the computing device.

22. (Original) The method of claim 1, further comprising the step of:

providing a graphical user interface (GUI) for allowing the user to organize the meta data

collection.

23. (Original) The method of claim 22, wherein the GUI displays a graphical tool in a cylindrical configuration for organizing the meta data collection.

24. (Cancelled)

25. (Previously Presented) The method of claim 88, wherein, in the encrypting step, the encryption key is represented as a hash of identifying information associated with the new segment, concatenated with a pass phrase of the user.

26. (Original) The method of claim 1, wherein the computing device implements a Common Data Security Architecture (CDSA), and the utilizing step is performed by a CDSA add-on module.

27. (Original) The method of claim 1, wherein the central repository subsystem is implemented using WebDAV protocols.

28. (Currently Amended) A computer program product embodied on computer readable medium readable by at least one of a computing device and a central repository subsystem, for managing meta data using a central repository at the central repository subsystem, the central repository being accessible by the computing device through a communication network, the computer program product comprising:

computer executable code configured to connect, through the communications network, to the central repository based on a user input;

computer executable code configured to update a local repository of the computing device with at least one segment from the central repository that is associated with the user to produce a meta data collection associated with the user; and

computer executable code configured to utilize, by the computing device, the meta data collection during a current user session at the computing device to assist the user in using the computing device,

wherein the computer executable code configured to utilize comprises computer executable code configured to retrieve, from the meta data collection, meta data that would be most appropriate for each of different contexts of using the computing device, based on at least a current role ~~position~~ of the user.

29.   (Previously Presented) The computer program product of claim 28, further comprising:

computer executable code configured to upload any new segment from the computing device to the central repository at a predetermined time.

30.   (Previously Presented) The computer program product of claim 28, further comprising:

computer executable code configured to incrementally upload any new meta data generated during the current user session from the computing device to the central repository.

31. (Previously Presented) The computer program product of claim 28, wherein the computer executable code configured to connect comprises:

computer executable code configured to receive, by the central repository subsystem, authentication information from the user;

computer executable code configured to verify validity of the authentication information; and

computer executable code configured to notify the computing device that the user has proper authority to access the central repository if the authentication information is verified as valid.

32. (Previously Presented) The computer program product of claim 31, wherein the authentication information comprises user identification, a pass phrase of the user, and an identifier for the central repository or a component at the central repository subsystem.

33. (Previously Presented) The computer program product of claim 32, wherein the computer executable code configured to verify comprises:

computer executable code configured to determine a secret key represented as a hash of:

the received user identification, concatenated with a hash of the received identifier, concatenated with the received pass phrase; and

computer executable code configured to compare the secret key with a stored key associated with the user.

34. (Previously Presented) The computer program product of claim 28, wherein the computer executable code configured to update comprises:

computer executable code configured to determine if the local repository is at a null state;

computer executable code configured to first request the central repository subsystem to transmit any segment associated with the user that has not been applied to the computing device if the local repository is not at a null state; and

computer executable code configured to second request the central repository subsystem to transmit all segments associated with the user if the local repository is at a null state.

35. (Previously Presented) The computer program product of claim 34, wherein the computer executable code configured to update further comprises:

computer executable code configured to receive at least one segment from the central repository subsystem in response to said first requesting instructions;

computer executable code configured to decrypt the at least one segment; and

computer executable code configured to apply the decrypted at least one segment to the meta data collection to produce the meta data collection associated with the user.

36. (Previously Presented) The computer program product of claim 34, wherein the computer executable code configured to update further comprises:

computer executable code configured to receive at least one segment from the central repository subsystem in response to said second requesting instructions;

computer executable code configured to decrypt the at least one segment; and

computer executable code configured to generate the meta data collection for the user using the decrypted at least one segment.

37.   (Previously Presented) The computer program product of claim 28, wherein the computer executable code configured to retrieve is implemented using heuristics algorithms and the computer executable code configured to utilize further comprises computer executable code configured to apply the retrieved meta data in each of the different contexts.

38.   (Previously Presented) The computer program product of claim 37, wherein the current context comprises at least one of the following: opening a web page, filling in a computer form, filling in a password-changing form, providing a certificate, opening a computer file, processing a computer file, or executing an application program.

39.   (Previously Presented) The computer program product of claim 37, wherein the computer executable code configured to utilize further comprises:

computer executable code configured to continuously collect meta data resulting from use of the computing device during the current user session at the computing device; and

the method further comprises:

computer executable code configured to generate a new segment based on the collected meta data upon completion of the current user session; and

computer executable code configured to process the new segment.

40.   (Previously Presented) The computer program product of claim 39, wherein the

computer executable code configured to process comprises:

computer executable code configured to update the meta data collection with the new

segment.

41.   (Previously Presented) The computer program product of claim 39, wherein the meta

data comprises application data for being usable in an application executable on the computing

device, and context data for identifying context in which said application data are used, and

wherein the computer executable code configured to utilize further comprises:

computer executable code configured to determine statistical information

associated with the meta data, the statistical information indicating relationships between

the meta data, wherein the computer executable code configured to retrieve is executed in

part based on the statistical information.

42.   (Original) The computer program product of claim 41, wherein the context data

identify at least one of the following: user roles, uniform resource identifiers (URIs), file names,

and/or form names pertaining to the application data.

43.   (Previously Presented) The computer program product of claim 41, wherein the

application data comprise at least one of the following: page display setting data, file display

setting data, user ID/password combinations, field values for computer forms, user's preference

data, bookmarks, and certificates.

44. (Previously Presented) The computer program product of claim 37, wherein the current context is for filling in a computer form, and the computer executable code configured to apply comprises computer executable code configured to automatically fill in the computer form with said most appropriate meta data.

45. (Previously Presented) The computer program product of claim 37, wherein, if the current context is for filling in a computer form, the computer executable code configured to utilize further comprises:

computer executable code configured to retrieve, from the meta data collection, alternative meta data that are related to the current context of filling in the computer form; and

computer executable code configured to present the alternative meta data to the user for the user's consideration.

46. (Previously Presented) The computer program product of claim 37, wherein the current context is for filling in a password-changing computer form, and the retrieved meta data comprises a user identification and a password, and

wherein the computer executable code configured to apply comprises:

computer executable code configured to present to the user the password in an obfuscated format;

computer executable code configured to determine whether it is safe to present the actual password to the user; and

computer executable code configured to present the actual password in a non-obfuscated format when it is determined to be safe to present the actual password.

47. (Previously Presented) The computer program product of claim 28, wherein the computer executable code configured to utilize comprises:

computer executable code configured to formulate search requirements based on a current context of using the computing device; and

computer executable code configured to execute a search based on the search requirements using heuristics algorithms.

48. (Original) The computer program product of claim 47, wherein the search requirements specify weighted properties of the current context of using the computing device.

49. (Previously Presented) The computer program product of claim 28, further comprising:

computer executable code configured to provide a graphical user interface (GUI) for allowing the user to organize the meta data collection.

50. (Original) The computer program product of claim 49, wherein the GUI displays a graphical tool in a cylindrical configuration for organizing the meta data collection.

51. (Cancelled)

52. (Previously Presented) The computer program product of claim 89, wherein the encryption key is represented as a hash of identifying information associated with the new segment, concatenated with a pass phrase of the user.

53. (Previously Presented) The computer program product of claim 28, wherein the computing device is configured in Common Data Security Architecture (CDSA), and the computer executable code configured to utilize is executed by an add-on module to the CDSA configuration.

54. (Original) The computer program product of claim 28, wherein the central repository subsystem is implemented using WebDAV protocols.

55. (Currently Amended) A system for managing meta data in a secure manner, the system comprising:

a central repository subsystem comprising a central repository for storing a plurality of segments associated with a user in a collection order; and

at least one computing device capable of communicating with the central repository subsystem through a communications network, the computing device comprising a local repository and being capable of connecting, through the communications network, to the central repository based on a user input, updating the local repository with at least one of the segments from the central repository to produce a meta data collection associated with the user, and

utilizing the meta data collection during a current user session at the computing device to assist

the user in using the computing device,

wherein the computing device retrieves, from the meta data collection, meta data that

would be most appropriate for each of different contexts of using the computing device, based on

at least a current role position of the user.

56. (Original) The system of claim 55, wherein the computing device uploads any new

segment to the central repository at a predetermined time.

57. (Original) The system of claim 55, wherein the computing device incrementally

uploads to the central repository any new meta data generated during the current user session.

58. (Previously Presented) The system of claim 55, wherein the computing device

further comprises:

a plurality of applications selectably executable on the computing device;

a security-service providing architecture structure for selectively providing security-based

services to at least one of the plurality of applications;

a data repository module, provided as an add-in module to the security-service providing

architecture, for utilizing the meta data collection to assist the user in using the computing

device; and

an encryption/decryption module for encryption any new segment to be transmitted to the

central repository subsystem.

59. (Previously Presented) The system of claim 55, wherein the central repository subsystem further comprises a manager for managing the central repository, and

wherein the central repository subsystem receives from the computing device authentication information input by the user, verifies validity of the authentication information, and notifies the computing device that the user has proper authority to access the central repository if the authentication information is verified as valid.

60. (Previously Presented) The system of claim 59, wherein the authentication information comprises user identification, a pass phrase of the user, and an identifier for the central repository or a component at the central repository subsystem.

61. (Previously Presented) The system of claim 59, wherein the central repository subsystem determines a secret key represented as a hash of:

the received user identification, concatenated with a hash of the received identifier, concatenated with the received pass phrase, and

the central repository subsystem compares the secret key with a stored key associated with the user to verify the user's authentication information.

62. (Original) The system of claim 58, wherein the data repository module determines if the local repository is at a null state, transmits a first request to the central repository subsystem to transmit any segment associated with the user that has not been applied to the computing device if the local repository is not at a null state, and transmits a second request to the central

repository subsystem to transmit all segments associated with the user if the local repository is at

a null state.

63. (Original) The system of claim 62, wherein the encryption/decryption module

receives at least one segment from the central repository subsystem in response to said first

request, and decrypts the at least one segment, and wherein the data repository module applies

the decrypted at least one segment to the meta data collection to produce the meta data collection

associated with the user.

64. (Original) The system of claim 62, wherein the encryption/decryption module

receives at least one segment from the central repository subsystem in response to said second

request, and decrypts the at least one segment, and wherein the data repository module generates

the meta data collection for the user using the decrypted at least one segment.

65. (Previously Presented) The system of claim 58, wherein the data repository module

retrieves the most appropriate meta data using heuristics algorithms and transmits the retrieved

meta data to an appropriate one of the applications which in turn applies the retrieved meta data

in each of the different contexts.

66. (Previously Presented) The system of claim 65, wherein the current context

comprises at least one of the following: opening a web page, filling in a computer form, filling in

a password-changing form, providing a certificate, opening a computer file, processing a computer file, or executing an application program.

67. (Original) The system of claim 65, wherein the data repository module continuously collects meta data resulting from use of the computing device during the current user session at the computing device, and generates a new segment based on the collected meta data upon completion of the current user session.

68. (Previously Presented) The system of claim 67, wherein the data repository module updates the meta data collection with the new segment.

69. (Previously Presented) The system of claim 67, wherein the meta data comprises application data for being usable in an application executable on the computing device, and context data for identifying context in which said application data are used, and

wherein the data repository module determines statistical information associated with the meta data and retrieves said appropriate meta data based on the statistical information, the statistical information indicating relationships between the meta data.

70. (Original) The system of claim 69, wherein the context data identify at least one of the following: user roles, uniform resource identifiers (URIs), file names, and/or form names pertaining to the application data.

71.   (Previously Presented) The system of claim 69, wherein the application data

comprises at least one of the following: page display setting data, file display setting data, user

ID/password combinations, field values for computer forms, user's preference data, bookmarks,

and certificates.

72.   (Original) The system of claim 65, wherein the current context is for filling in a

computer form, and said appropriate one of the applications automatically fills the computer

form with said most appropriate meta data.

73.   (Original) The system of claim 65, wherein, if the current context is for filling in a

computer form, the data repository module retrieves, from the meta data collection, alternative

meta data that are related to the current context of filling in the computer form, and transmits the

alternative meta data to said appropriate one of the applications which in turn presents the

alternative meta data to the user for the user's consideration.

74.   (Previously Presented) The system of claim 65, wherein the current context is for

filling in a password-changing computer form, and the retrieved meta data comprises a user

identification and a password, and wherein the data repository module controls said appropriate

one of the applications to present to the user the password in an obfuscated format, determines

whether it is safe to present the actual password to the user, and controls said appropriate one of

the applications to present the actual password in a non-obfuscated format when it is determined

to be safe to present the actual password.

75. (Previously Presented) The system of claim 58, wherein the data repository module formulates search requirements based on a current context of using the computing device, and executes a search based on the search requirements using heuristics algorithms.

76. (Original) The system of claim 75, wherein the search requirements specify weighted properties of the current context of using the computing device.

77. (Original) The system of claim 55, further comprising:

a meta data editor for allowing the user to organize the meta data collection.

78. (Original) The system of claim 77, wherein the meta data editor displays a graphical tool in a cylindrical configuration for organizing the meta data collection.

79. (Cancelled)

80. (Previously Presented) The system of claim 90, wherein the encryption key is represented as a hash of identifying information associated with the new segment, concatenated with a pass phrase of the user.

81. (Original) The system of claim 58, wherein the computing device is configured in Common Data Security Architecture (CDSA), and the data repository module is an add-on module to the CDSA configuration.

82. (Original) The system of claim 55, wherein the central repository subsystem is implemented using WebDAV protocols.

83. (Original) The system of claim 55, wherein at least one of the central repository and the local repository is implemented using a network-attached storage.

84. (Original) The system of claim 58, wherein the data repository module resides on a proxy machine accessible through a predetermined connection means.

85-87. (Cancelled)

88. (Previously Presented) A method of managing meta data using a central repository at a central repository subsystem, the central repository being accessible by a computing device through a communications network, the method comprising the steps of:

connecting to the central repository through the communications network based on a user input;

updating a local repository of the computing device with at least one segment from the central repository that is associated with the user to produce a meta data collection associated with the user;

utilizing, by the computing device, the meta data collection during a current user session at the computing device to assist the user in using the computing device; and

uploading any new segment from the computing device to the central repository at a predetermined time,

wherein the uploading step comprises:

temporarily locking the local repository;

encrypting the new segment using an encryption key;

transmitting the encrypted new segment from the computing device to the central repository subsystem for storage in the central repository; and

unlocking the local repository.

89. (Previously Presented) A computer program product embodied on computer readable medium readable by at least one of a computing device and a central repository subsystem, for managing meta data using a central repository at the central repository subsystem, the central repository being accessible by the computing device through a communication network, the computer program product comprising:

computer executable code configured to connect, through the communications network, to the central repository based on a user input;

computer executable code configured to update a local repository of the computing device with at least one segment from the central repository that is associated with the user to produce a meta data collection associated with the user;

computer executable code configured to utilize, by the computing device, the meta data collection during a current user session at the computing device to assist the user in using the computing device; and

computer executable code configured to upload any new segment from the computing

device to the central repository at a predetermined time,

> wherein the computer executable code configured to upload comprises:

>> computer executable code configured to temporarily lock the local repository;

>> computer executable code configured to encrypt the new segment using an

encryption key;

>> computer executable code configured to transmit the encrypted new segment from

the computing device to the central repository subsystem for storage in the central

repository; and

>> computer executable code configured to unlock the local repository.

90. (Previously Presented) A system for managing meta data in a secure manner, the

system comprising:

a central repository subsystem comprising a central repository for storing a plurality of

segments associated with a user in a collection order; and

at least one computing device capable of communicating with the central repository

subsystem through a communications network, the computing device comprising a local

repository and being capable of connecting, through the communications network, to the central

repository based on a user input, updating the local repository with at least one of the segments

from the central repository to produce a meta data collection associated with the user, and

utilizing the meta data collection during a current user session at the computing device to assist

the user in using the computing device,

wherein the computing device further comprises:

a plurality of applications selectably executable on the computing device;

a security-service providing architecture structure for selectively providing security-based services to at least one of the plurality of applications;

a data repository module, provided as an add-in module to the security-service providing architecture, for utilizing the meta data collection to assist the user in using the computing device; and

an encryption/decryption module for encryption any new segment to be transmitted to the central repository subsystem, and

wherein the data repository module temporarily locks the local repository and creates the new segment based on collected meta data, the encryption/decryption module encrypts the new segment using an encryption key, and the data repository module transmits the encrypted new segment to the central repository subsystem for storage in the central repository and unlocks the local repository.

91. (New) The method of claim 1, wherein the meta data collection stored in the local repository of the computing device at the user's side includes a plurality of meta data groups, each of the meta data groups corresponding to one of a plurality of roles of the user.

92. (New) The computer program product of claim 28, wherein the meta data collection stored in the local repository of the computing device at the user's side includes a plurality of

meta data groups, each of the meta data groups corresponding to one of a plurality of roles of the user.

93. (New) The system of claim 55, wherein the meta data collection stored in the local repository of the computing device at the user's side includes a plurality of meta data groups, each of the meta data groups corresponding to one of a plurality of roles of the user.